ARMY RESEARCH LABORATORY

Vulnerability Assessment of the InterNetwork Controller (INC)

by Charles Retter
and Douglas Gwyn

ARL-MR-412 September 1998

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

Abstract

The Tactical Internet (TI) provides a reliable digital communications infrastructure for Task Force XXI at brigade level and below. The InterNetwork controller (INC) performs routing and protocol conversion of data traffic within the TI, so its vulnerabilities could have significant adverse effects on the flow and content of data communications within the TI. This report summarizes the results of a study of potential "information warfare" vulnerabilities of the INC's interfaces, configuration, protocols, procedures, and policies.

Table of Contents

List of Figures

INTENTIONALLY LEFT BLANK.

1 Introduction

The Tactical Internet (TI) provides a reliable digital communications infrastructure for Task Force XXI at brigade level and below [1]. It includes a variety of communications and routing units, interconnected according to the command structure [2]. Since these interconnections may change quickly during the course of a battle, the routing units must be able to respond to changes in network configurations. Figure 1 shows a typical configuration of some of the communication and routing units below the brigade level. At the lowest level, an individual soldier can be equipped with a hand-held (HH) single-channel ground/air radio system (SINCGARS) System Improvement Program (SIP) radio and a dismounted soldier system unit (DSSU). SINCGARS radios are capable of both voice and data transmission and are used for both command and control (C^2) and situation awareness (SA) data. The routing functions at this level are handled by a lightweight InterNetwork controller (LINC). At the company level, larger SINCGARS SIP radios are used; the standard InterNetwork controller (INC) can handle the routing for two of these plus an enhanced position location and reporting system (EPLRS) digital radio for communications in the wide-area network used at higher levels. The battalion would also have EPLRS radios with INC routers but, in addition, would have tactical message gateways (TMG), which handle multiple protocols and provide network reachability information between different parts of the network [3]. An *appliqué* host may be used in conjunction with the INC to support network application software and to override the normal domain-based hostname-to-address mapping.

Since the INC performs routing and protocol conversion of data traffic within the TI, its vulnerabilities could have significant adverse effects on the flow and content of data communications within the TI. Thus, it is important to identify the most readily exploitable vulnerabilities in the INC (and in the overall TI architecture) and to propose methods to reduce their impact.

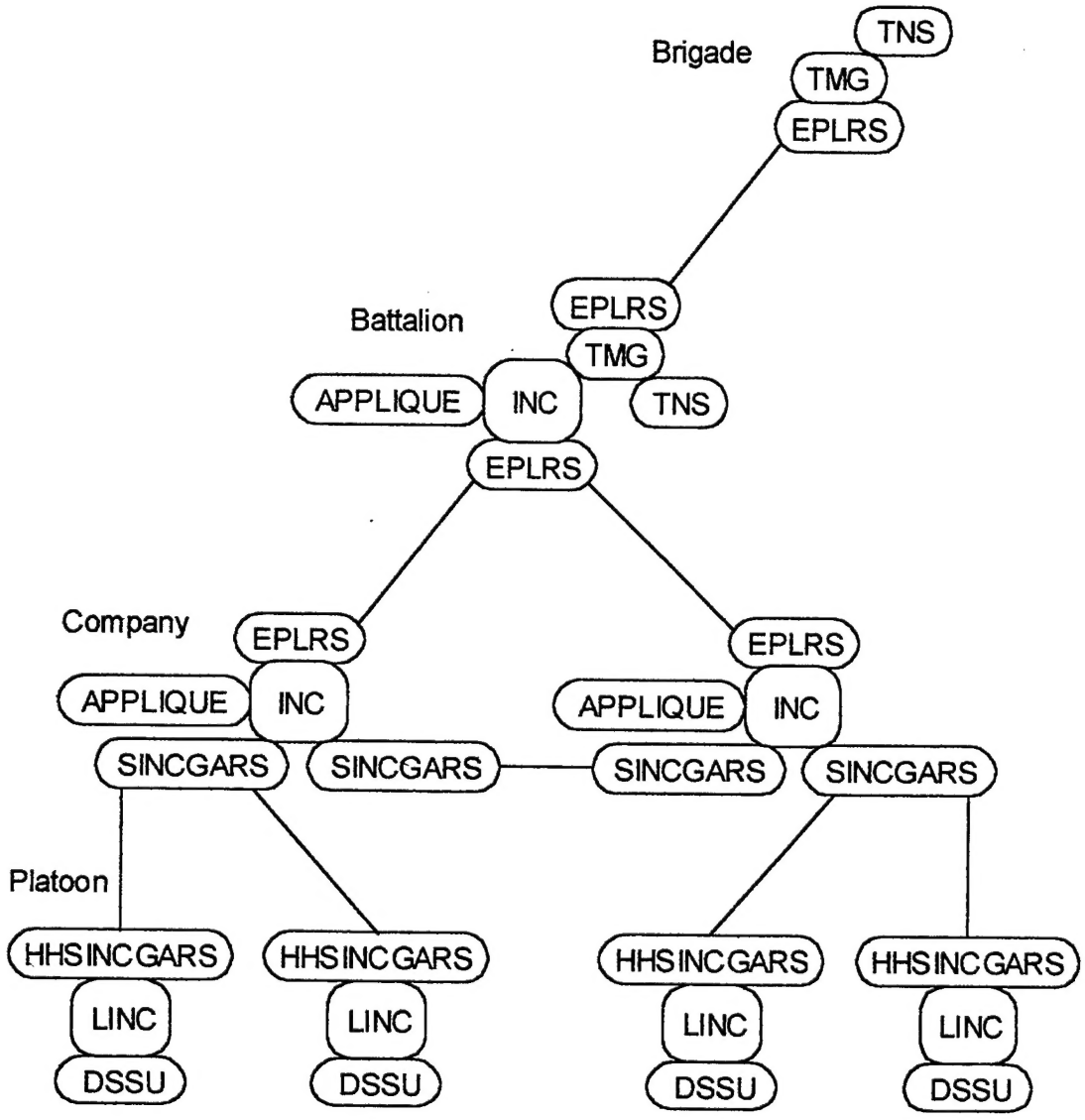

Figure 1. Typical router connections in the TI.

2 Scope of Work

This report summarizes the results of a study of potential "information warfare" vulnerabilities of the INC's interfaces, configuration, protocols, procedures, and policies. Since the standard protocols used to interchange information among Internet hosts have been thoroughly analyzed elsewhere [4, 5, 6] and, indeed, are scheduled to be supplanted by more secure protocols within a few years [7], we are not attempting to exhaustively catalog all security defects in the standard Internet protocols. Instead, we concentrate on the most pervasive weaknesses in the context of the TI (which imposes more limits on access than does the commercial Internet) and on characteristics unique to the INC and its operational environment.

3 Network Security

3.1 Security Services

We can identify six major security requirements for general communication networks [4, 8].

(1) **Confidentiality** Unauthorized parties ("eavesdroppers") must not be able to obtain significant information from intercepted data. We also may refer to this as *secrecy*.

(2) **Authentication** The origin of data must be reliably identified.

(3) **Integrity** The content of data must be reliably controlled by authorized parties only.

(4) **Access Control** The target host must be able to control access to its data resources.

(5) **Availability** Data and other services must be available to authorized parties when needed. This implies that communication channels must be available.

(6) **Nonrepudiation** A third party can verify that a particular message was transmitted, despite denials by sender or receiver.

All of these security services are clearly relevant to achievement of military objectives via the TI, except for nonrepudiation, which is typically used for financial transactions. We give here examples of possible adverse consequences of failure for the others.

(1) **Confidentiality** Enemy eavesdroppers (a.k.a. "intercept operators") can obtain information of value to enemy planners that is otherwise unavailable to them, such as the condition of our vehicles or location and morale of our troops, thereby improving the enemy's ability to exploit our weaknesses and to avoid confronting our strengths.

(2) **Authentication** The enemy can issue false orders in order to reposition our units in a configuration more vulnerable to attack, and subordinate units will obey the orders, while their superiors can similarly be misinformed about the disposition of their subordinate units.

(3) **Integrity** Location information, inventory, etc., within an SA can be changed so that a unit's superior makes decisions based on false information, which results in degraded readiness that can be exploited by enemy action.

(4) **Access Control** The enemy can steal or falsify mission-critical information, and can withhold it from authorized units.

(5) **Availability** Orders can be blocked so that coordination among units suffers, while prevention of delivery of SAs increases the likelihood of "friendly fire" casualties.

3.2 Security Threats

There are four major threats to the intended flow of information from authorized source to destination [4].

(1) **Interruption** An asset of the network becomes unavailable or unusable (which adversely affects availability).

(2) **Interception** An unauthorized party, in our case a presumed enemy agent, gains access to secret information, either data content or operational information via *traffic analysis* [9]. (This is a compromise of confidentiality.)

(3) **Modification** The enemy obtains the ability to control some portion of the contents of data transmitted over the network (which compromises integrity).

(4) **Fabrication** An unauthorized party transmits false identity information (which violates authenticity) in conjunction with counterfeit data, which is thus accepted by the recipient as genuine.

Both interception and fabrication attacks can be used to obtain unauthorized access to controlled resources.

Threats can also be categorized [4] as *passive* (i.e., based on eavesdropping or relaying without blocking delivery of the data) or *active* (i.e., based on sending information at least part of which is created by the enemy agent).

Passive attacks include the following.

(1) **Release of Data** Message contents are visible to the attacker.

(2) **Traffic Analysis** The nature of the communication, or of the organization whose units are communicating, is determined from communication characteristics such as accessible hosts and frequency of contact [9].

Active attacks include the following.

(1) **Masquerade** An unauthorized entity pretends to have the identity of an authorized entity. This facilitates the use of other active attacks.

(2) **Replay** Previously captured communications are later retransmitted to achieve an unauthorized effect (such as a formerly benign effect at an inopportune moment).

(3) **Modification** A portion of a legitimate message is altered to achieve an unauthorized effect.

(4) **Denial of Service** Normal use or management of communications is prevented or disrupted.

Defense against passive attacks generally consists in taking preventive measures such as encryption of message contents, while defense against active attacks consists primarily of detection; when an intruder's activities are detected, often remedial action can be taken to recover from the disruption and delays caused by the attack. Enemy knowledge that active attacks can be detected may also help to prevent them.

4 Assumed Threat Context

We assume that normal military communication security measures (COMSEC) will be implemented to protect TI physical information channels, at least for those channels most susceptible to outside interference and interception, such as radio links. We also assume that local, direct connections such as are used among equipment within an integrated platform will not employ encryption, in order to avoid the attendant drawbacks when there would be little apparent gain for encrypting internal channels.

In such circumstances, the most significant avenues of attack against the TI by an enemy agent would be (1) interference with delivery (e.g., by jamming that causes loss of a significant amount of data traffic on one or more links) and (2) capture of an intact, functioning TI station (including unencrypted local links) with consequent ability to intercept traffic directed to that unit, to masquerade as that unit, and to modify the

information sent from that unit. In addition, any connection between the TI and the commercial Internet [1, §6.2] would raise the possibility that packets from anywhere in the world might be routed into the TI, leading to undesirable congestion of the network or even more significant problems. Since no connection with the commercial Internet is planned for the Task Force XXI brigade experiment, we will consider only the threats from jamming and node capture.

4.1 Jamming

Without analyzing details of the actual implementation of frequency-hopping spread spectrum technology in the SINCGARS SIP communication link, it is still apparent that a sufficiently high level of jamming must result in some corruption of data. Because most Internet services utilize *reliable* protocols, this would cause retransmission of data packets that are detected to be invalid (generally as the result of a checksum failure), in effect delaying delivery of information. Indeed, it is clear that beyond a certain bit-loss rate threshold, such communications involving reliable protocols would have drastically reduced effective throughput, because the Internet error-correction protocol acts as a multiplier of the bit-loss rate (a single corrupted bit causes an entire data packet to be discarded). This points up the desirability of designing error-correction schemes to take into account properties of the entire communication path, rather than layering separate error-control protocols on each other as occurs when Internet protocols are embedded within the SINCGARS SIP coded tunnel. When effective throughput becomes insufficient to transmit all necessary data, a successful denial-of-service attack has occurred.

In order to keep this report unclassified, we have made no attempt to determine the exact degree of susceptibility of SINCGARS SIP or EPLRS transmissions to hostile jamming activity. However, we note that this is an obvious avenue of attack and that it deserves further study.

4.2 Node Capture

Without analyzing details of the cryptologic protocols such as ability of a superior unit to revoke credentials for a compromised station, we acknowledge the possibility that, in an active conflict, a station and its crypto keys, schedules, operational staff, etc. may be suddenly seized and pressed into continued service in order to serve the enemy's agenda for as long as the seizure remains undetected by other units. (This is a form of masquerade attack.) The aspect of this standard military COMSEC issue that is especially relevant for the current study is the impact that such a compromised site may have on communications within the TI other than those directed to or from the particular site. Specifically, we need to consider whether the site will be able to interfere with communications among other hosts on the network. Because of the presence of unencrypted direct connections to an INC, there is ample opportunity for the enemy to insert data packets of his own choosing into the network and the potential

for such packets to be routed to the rest of the TI over the encrypted links. For example, the enemy could possess a portable computer loaded with his own software capable of inserting appropriate attack packets into the network; alternatively, the operational software in the INC might be replaced (via the initial program load facility) with such software. This scenario (node capture and exploitation) will be adopted as the "worst-case" context within which we assess INC vulnerability.

While some of the uses an enemy might make of a captured node are obvious, more subtle ones might be overlooked. There are two obvious approaches to take advantage of a captured node.

(1) Use it passively to watch what is happening on the network, either decrypting messages if the appropriate keys are available, or for traffic analysis.

(2) Use it actively to insert new information, routing commands, etc.

The first has the advantage of being harder to detect, so it may be useful for longer periods of time, while the second could potentially cause more damage, especially if done at the right time, or if it somehow remains undetected. Because of the significance of detecting such node captures, an enemy might want to try approaches in between (1) and (2).

For example, if a node that contains the frequency-hopping sequence used by a group of SINCGARS radios is captured, it could be used as a much more effective jammer than a transmitter that does not know the sequence being used, especially if the node is combined with a large amplifier and/or a high-gain antenna. Simply jamming all transmissions would quickly be detected and the other radios would switch to a new sequence. However, suppose that the captured node were used very selectively to interfere with just enough data packets to cause the network to be congested with retransmissions. This kind of interference seems much less likely to be recognized as a jamming problem. In fact, by timing the interference properly, it might be possible to make it appear that the problem was another node in the network, rather than the one that had been captured. If the captured node were being used as a router, it might be possible to interfere with an alternate router, resulting in more traffic being directed to the captured node.

This suggests a general form of attack: use the captured node to insert signals or data that will be handled automatically by the network protocols, and not come to the attention of humans. We assume that normal procedures will eventually reveal that the node has been captured, but considerable damage could be done before that, and tracing and repairing the damage might be infeasible, especially in the tactical environment.

There are three general categories of potential vulnerabilities to captured nodes.

(1) **Protocol Weaknesses** These are properties of the Internet protocols as used within the TI, generally due to insufficient attention to security requirements when the protocols were designed [5].

(2) **Implementation Errors** These result from inadequacies in implementation of the protocols and may be considered as "bugs" that could be fixed by relatively small changes to software. Most of the well-known "CERT advisories" fall into this category.

(3) **Policy Weaknesses** These pertain to improper employment of the protocols. For example, inappropriate power to reconfigure the network topology might be granted to subordinate units.

5 Internet Protocols

For interoperability, the INC software implements several fundamental data transfer and system management protocols that are defined by existing Internet standards. Among these are the following.

IP Internet Protocol — a general information-packetizing protocol used to encapsulate higher-level protocols that require reliable transmission of information. IP packets for a given data connection might be relayed from host to host until they reach their addressee; such *routing* can send portions of the data through different paths (routes) [RFC-791].

TCP Transmission Control Protocol — a data-transmission protocol based on IP that provides a reliable, full-duplex *virtual circuit* between communicating hosts [RFC-793].

UDP User Datagram Protocol — used for noncrucial update information that can be "discarded" (fail to be received by its intended destination host) without notification [RFC-768].

ICMP Internet Control Message Protocol — a low-level method for controlling and monitoring TCP and UDP connections [RFC-792].

FTP File Transfer Protocol — a protocol based on TCP/IP used to transfer entire files [RFC-759].

TFTP Trivial File Transfer Protocol — a protocol similar to FTP, but without authentication checks. TFTP is typically used to *bootstrap* load an initial file system when a diskless host begins operation, after which files needed for authenticating the host will be available [RFC-783].

OSPF Open Shortest Path First — a routing protocol that is used to maintain a map of the dynamic network topology, so that packets will be sent via the *shortest path* (fewest number of relays) available [RFC-2328].

SNMP Simple Network Management Protocol — used to initialize and reconfigure connectivity information (Management Information Bases [MIB]) [RFC-1157, RFC-1213].

ARP Address Resolution Protocol — a broadcast protocol used to query hosts to obtain their specific low-level connection identification codes. While Internet hosts could be addressed by such hardware-specific codes, instead the standard Internet protocols employ uniform *IP addresses,* which are (currently 32-bit) numeric host-interface identifiers assigned in a coordinated scheme so that, ideally, each host in the universe has its own unique IP address. ARP broadcasts the IP address and listens for a host that recognizes it to respond with its hardware address, which can then be used to communicate privately with the host [RFC-826].

PPP Point-to-Point Protocol — a method for transporting datagrams over point-to-point links, such as serial lines [RFC-1661, RFC-2153].

IPCP Internet Protocol Control Protocol — a network control protocol for establishing and configuring IP over PPP [RFC-1332].

While IP addresses (e.g. `128.63.18.87`) are the fundamental method of host identification on the Internet, for human convenience more mnemonic *host names* (e.g. `STYRENE.ARL.MIL`) are generally used to designate hosts. A hierarchical database, distributed across the Internet according to a *domain* structure, that associates host names with IP addresses has been established using the following protocol.

DNS Domain Name Service — used to map host names to IP addresses or sometimes vice-versa, capable of having portions of the host-name space administered in local *domains* rather than centrally for the whole Internet [RFC-1034, RFC-1035].

6 TI-Specific Protocols

The INC also implements some protocols not commonly encountered on the public Internet, including MIL-STD-188-220B [10], which is a family of protocols used by digital message transfer devices (DMTD), which are essentially modems or data buffers used with SINCGARS/SIP and similar radio equipment. Internet protocols are implemented on top of this interface.

Of interest for any vulnerability assessment of TI routing is an *appliqué* host being supplied for the Task Force XXI experiment, which is used to map relatively static host names such as "commander" to the more dynamic host names that reflect actual equipment nodes. The intent is to allow communication with significant units, such as the commander, regardless of which actual host happens to be attached to the unit at that moment. (This does not strike us as an optimal solution to the *mobile computing*

issue, but it is a potentially vulnerable component of Task Force XXI's TI design.) This *appliqué* system in effect provides an additional layer of name mapping wrapped around the DNS mapping and, thus, an additional avenue of attack during information warfare.

7 Protocol Weaknesses

The Internet, originally the ARPAnet, was designed to automatically route information despite dynamic changes in network topology, such as would result from an enemy attack taking out some relay sites. Some essential components of the Internet design are the use of *packets* to encapsulate data, the distribution of routing information (host identity, connectivity, bandwidth, etc.) across the network, and hierarchical organization into *subnets*.

The original emphasis was on providing good connectivity, rather than on secure communications. Consequently, as the Internet has evolved from a research platform into the essential commercial utility that it now is, some security weaknesses in the early Internet protocols have become evident. While most attention has been focused on the public Internet, many of the problems identified in that context are also relevant in our assumed TI scenario wherein a node falls under enemy control.

The main difference in security considerations for the TI context vs. the public Internet is that we must concentrate on *insider* attacks, due to node capture, rather than attacks originating in outside subnetworks. Therefore, commonly proposed solutions such as firewalls [6] are not as useful for the TI as they are for the public Internet. Of course, if the TI is eventually connected to the public Internet via some gateway (pursuant to the "split-base" doctrine), the problems discussed in Cheswick and Bellovin [6] would have to be addressed, since rogue packets entering the network are undesirable even when secure encryption is being used.

8 General Internet Security Problems

As previously mentioned, existing Internet communication relies largely on protocols that were not designed with security in mind; these include most of the protocols specified for the INC. In particular, many applications trust that the sender's IP address, contained within the header of a received IP packet, is authentic. However, it is not too hard for a knowledgeable person with physical access to the transmission medium anywhere along the routing path to forge IP packets that contain fake sender IDs; any recipient that trusts the sender IP address is said to have been *spoofed*. Acting on information so received obviously constitutes a significant security problem. Absent any reliable authentication mechanism at the IP (or a logically more basic) level, it is difficult to guard against such problems. In a previous study [11], we demonstrated how, with specially formatted messages, secure communication could be

embedded within such an insecure transport mechanism, but the vast majority of existing applications do not implement such a scheme and are thus inherently vulnerable to spoofing.

Rampant exploitation of such weaknesses in existing Internet protocols, combined with the imminent depletion of available 32-bit IP addresses, has led to a concerted effort by the Internet Engineering Task Force to design replacement protocols that incorporate significant security features from the outset. For instance, IPv6 [RFC-1883] is slated to replace the current IP protocol (IPv4). (Also, see Hinden [7].) IPv6 includes embedded support for reliable host authentication [RFCs 1825–1829]. However, hosts that understand only IPv4 are likely to remain on the public Internet for many years, and it is likely that fielded military systems will support IPv4 for some time. The newer protocols, if they prove successful, would probably be worth adoption for the TI and similar Internet-based military networks, as a relatively economical way to implement this basic level of authentication. There are key-management issues associated with the new Internet protocols that deserve careful study, particularly in the military context where COMSEC measures may already solve some of these issues.

There are many other well-known security problems with current Internet protocols, sometimes related to deficiencies in specific implementations (which are often derived from a single original implementation) and sometimes inherent in the protocols themselves. Bellovin [5] discusses attacks on various protocols, including ways to anticipate sequence numbers in protocols that use them for error control. IP address spoofing is an important example that we will take as representative of this class of problem.

A related problem has appeared recently on the commercial Internet [12]. The handshaking mechanism used to establish TCP connections with servers on the Internet involves three steps.

(1) The client sends a `SYN` packet to the server, requesting a connection.

(2) The server responds with a `SYN-ACK` packet.

(3) The client responds with an `ACK` packet.

Between the time that the `SYN-ACK` packet is sent and the time that the `ACK` packet is received, the connection is said to be *half-open.* Unfortunately, existing implementations can handle only a small number of half-open connections. Recently, commercial servers have been attacked by large numbers of `SYN` packets containing spoofed source addresses that do not correspond to any real machine. Since nothing responds to the `SYN-ACK` packets, the server quickly finds itself with too many half-open connections and either refuses real connections or crashes.

9 Network Administration

The Internet standard protocol SNMP is used to manage connections in each INC. In addition to local management at each INC, the eventual intent past Task Force XXI appears to be to allow SNMP management of INC connections from remote hosts that are specially designated as authorized to do so. The January 1996 draft of the *Tactical Internet System Concept Document* [2] specifies that:

> Network management of the INC is required. SNMP Version 1.0 and Management Information Base (MIB) Version 2.0 along with enterprise MIB extensions to support other protocols, interfaces, and functions not supported by MIB Version 2.0, are used to initialize, monitor, and control the INC based on changing mission needs. The INC hosts an SNMP agent. An NMS located in the attached host or elsewhere in the TI, interacts with the SNMP agent to access and control MIB variables.

SNMP Version 1.0 [RFC-1157] and MIB-II [RFC-1213] provide almost no security. That is, there is no significant authentication of the source of management messages and no way to prevent eavesdropping. There is a community name in the message header, but that can simply be copied from a previously observed message. Because of these weaknesses, there have been two major incompatible improvements to SNMP; a secure modification of SNMPv1 was created in 1992 [RFCs 1351–1353], and Version 2 of SNMP was issued in 1993 [RFCs 1441–1452], and revised in January 1996 [RFCs 1902–1910]. These newer protocols include real authentication, encryption of messages, and provisions to detect modification, replay, and reordering of messages. Version 2.0 also includes enhancements unrelated to security. Unfortunately, all three versions are incompatible with each other.

We tentatively conclude that the TI as currently specified is susceptible to interference via unauthorized network reconfiguration using the SNMP protocol.

10 Unauthorized Rerouting

From the foregoing analysis, we conclude that an attack from a captured node could, either once and for all with a single SNMP session or for each packet in data-transfer protocols (e.g., TCP and FTP), cause packets to be routed to or from unauthorized sources. Note that the use of encryption on each link does not prevent this kind of attack; the problem is that the Internet routing protocols operate automatically, and, indeed, this is essential to meet the design goal of network robustness. In traditional military radio networks of World War II – Korean War vintage, the ability to communicate with other units was constrained by possession of authorized cryptonet keys [9]; any attempt to relay information to a unit that one was not authorized to contact directly would necessarily be reviewed by a human, who would judge the

appropriateness of the relay request. This safety net has been removed with the advent of automatic routing.

The *Tactical Internet System Concept Document* [2] specifies that "The dynamic IP routing protocol OSPF Version 2.0 is used to support dynamic updating of IP routing tables with other IP routers (within the same AS) in the TI (e.g. other INCs and TMGs)." OSPF Version 2.0 [RFC-2328] includes an authentication field, but it normally contains a password shared by all of the routers in the area. This would allow a captured router to modify the routing tables in other routers in that area. The protocol provides for other authentication mechanisms, but does not specify them. The Interface Control Document for the INC–TMG Interface specifies simple password authentication [3, §3.6.2.3.1.7].

To reduce both accidental (friendly unit abusing excessive power to reconfigure remote parts of the network) or deliberate (enemy working from a captured node) abuse of access privileges, networks such as the TI should incorporate access control policy enforcement, for example by packet filtering (at least for SNMP traffic) similar to that provided by firewall systems [6]. In principle, packet filtering can be added to any implementation of the Internet protocols; a separate computer is not required. There are limits to the effectiveness of such techniques, however, in the absence of reliable authentication mechanisms. Typically, firewalls rely on IP addresses and possibly DNS to authenticate requests, and, as we have noted, these are subject to spoofing by an attacker. Therefore, access enforcement using some form of strong authentication (perhaps tied into the cryptographic system in use for encrypting communication links) is recommended.

11 *Appliqué* Name Mapping

Remote registration of `CNAME` resource records is required by the *Tactical Internet System Concept Document* [2, p. 39]. These records are used to map relatively static host names such as "commander" to the more dynamic host names that reflect actual equipment nodes. Each *appliqué* host on the TI must be capable of changing its mapping records in response to remote requests because the mappings may change rapidly and quick response to changes is necessary. Furthermore, each *appliqué* host is capable of being used as a name server, so that name server traffic can be dispersed toward lower levels of the net. This suggests that an attacker with a captured node could promulgate false mappings in remote *appliqués* as a way to achieve rerouting. Preventing this requires some form of authentication. Note that authentication of the immediate source of a mapping may not be sufficient. If the captured node was already operating as a name server, it might be accepted as a valid source when it provides a false mapping. In that case, some authentication of the mapping itself would be required to detect the deception. For example, the mapping might be encrypted with a public-key system for which only the commander has the encryption key, but all of the name servers have decryption keys. This would allow any name

server to verify the mapping, but not to generate new mappings. Some protection against replay attacks, such as sequence numbers, would also be required. A detailed study of *appliqué* exploitation is available as a separate classified report [13].

12 Implementation Errors

We do not consider it feasible in today's state of the programming art to produce a "provably correct" implementation of the Internet protocols. There are undoubtedly bugs in any such large software product. It was through exploitation of several such implementation deficiencies that the infamous "Internet worm" of 2 November 1988 [14] was able to propagate itself to thousands of hosts on the public Internet and severely disrupt network operation for several days. (It could have done even more damage, but its creator denies that that was his intent.) Clearly, it is important to eliminate exploitable implementation errors as quickly as they are discovered, and this can be facilitated by a friendly "tiger team" that ideally would have access to source code for the INC software. However, it must be acknowledged that an attacker could discover the existence of some such vulnerability before the tiger team does; an important implication of this is that *powers granted to TI nodes should be limited to the minimum necessary to achieve objectives.* This policy would limit the extent of potential damage should a functional node fall into enemy hands. Furthermore, it would increase the probability of detecting such a captured node if the enemy attempted to use it for some function that the node is not normally required to perform.

We have not examined the INC source code to locate such deficiencies, since that is an open-ended task better addressed by establishment of a tiger team in perpetual support of operations (and also by enemy information warfare departments!).

13 Policy Weaknesses

For purposes of the Task Force XXI experiment, several security policies are specified, most of them involving use of simple passwords to control access to various aspects of the network [3, §3.6.2.3.1.7]. Other operational procedures are specified that also have security ramifications.

The use of a shared password to administer network connectivity, including links not directly involving the particular node, is convenient for experimental purposes, but would be risky policy if implemented in the field; in case of node capture, this would permit the enemy to change routing so that data is not properly delivered, resulting in denial of service.

14 Authentication

As previously stated, the powers granted to a TI node should be limited to those necessary to achieve its objectives. Implementation of this limitation requires secure authentication. For example, suppose that one node in a network is allowed to reconfigure the routing tables on a distant router and its reconfiguration messages pass through a node that is not permitted to reconfigure the router. Then, the authentication mechanism should be able to detect the following types of problems.

(1) Messages that do not get through.

(2) Messages that are copies of previous valid messages.

(3) Messages that have been modified.

(4) Messages sent by the node without permission.

(5) Messages sent by one node pretending to be another node.

The first problem must be detected by the sender of the message when it fails to receive an acknowledgment (and the acknowledgment must also be authenticated, of course). The second problem, at least in cases where it is a problem, can be solved with time stamps or sequence numbers within the message, or by a challenge–response approach. The third problem, authentication of the data, is normally solved by computing a one-way hash function of the data and appending it or by using a cryptographic checksum. Finally, the identity of the source can be verified if a cryptographic signature is part of the message.

Authentication of the source and integrity of messages is a standard military function. The tactical end-to-end encryption device (TEED), planned to be used with the TI, encrypts and authenticates messages and provides multilevel security for users. However, the messages of interest in this study are communications between software agents, which also must be authenticated. At the level of network management, version 1 of SNMP has no provision for secure authentication, but version 2 does. To avoid the problems described previously, routers should use version 2 of SNMP with a secure authentication mechanism. However, before attacks like source-address spoofing are able to disrupt the network by causing congestion or other denial-of-service problems, they must be detected at a lower level. This may require the use of IPv6.

15 Conclusions

The InterNetwork Controller is the primary low-level router for the TI. This report has summarized the results of a study of potential "information warfare" vulnerabilities of the INC's interfaces, configuration, protocols, procedures, and policies. The most

significant form of attack we discussed is the use of a captured node to insert packets into the network. In the absence of reliable authentication, such packets could cause considerable disruption of the network, by modification of routing tables in other routers, flooding the network with useless packets, causing buffer overflows in other machines, etc. Secure authentication should be used both at the IP level (to avoid attacks like source-address spoofing) and at higher levels (to avoid improper use of SNMP, for example). Even if secure authentication is used, some disruption may be possible if no one knows that the node has been captured. For this reason, it is also important to contain the potential damage by limiting the capabilities of nodes as much as possible.

References

1. Army Digitization Office. *Army Digitization Master Plan '96.* Washington, DC, 1996 (available through `http://www.ado.army.mil/ADMP/1996/TOC.htm`).

2. *Tactical Internet System Concept Document.* Draft, January 1996.

3. *Interface Control Document (ICD) for the VAA Internet Controller (INC) to Tactical Multinet Gateway (TMG) Interface.* ITT, 30 June 1995 (ITT document number 1570647).

4. Stallings, W. *Network and Internetwork Security: Principles and Practice.* Prentice-Hall, 1995 (ISBN 0–02–415483).

5. Bellovin, S. M. "Security Problems in the TCP/IP Protocol Suite." *Computer Communication Review,* vol. 19, no. 2, pp. 32–48, April 1989 (available through `ftp://ftp.research.att.com/dist/internet_security/ipext.ps.Z`).

6. Cheswick, W. R., and S. M. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker.* Addison-Wesley, 1994 (ISBN 0–201–63357–4).

7. Hinden, R. M. "IP Next Generation Overview." *Communications of the ACM,* vol. 39, no. 6, pp. 61–71, June 1996.

8. Stallings, W. *SNMP, SNMPv2, and CMIP: The Practical Guide to Network Management Standards.* Addison-Wesley, 1995 (ISBN 0–201–63331–0).

9. Callimahos, L. D. *Traffic Analysis and the Zendian Problem — An Exercise in Communications Intelligence Operations.* Aegean Park Press, 1989 reprint (ISBN 0–89412–161–8).

10. U.S. Department of Defense. *Interoperability Standard for Digital Message Transfer Device Subsystems.* MIL-STD-188-220B, Washington, DC, 20 January 1998 (available through `http://www.itsi.disa.mil/`).

11. Broome, B., B. Cooper, D. Gwyn, and C. Retter. "Thwarting Intrusion in Network Protocols." U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, 1995, unpublished project report.

12. Computer Emergency Response Team. *CERT Advisory CA–96.21 — Topic: TCP SYN Flooding and IP Spoofing Attacks.* 14 November 1997 (available through `ftp://info.cert.org/pub/cert_advisories`).

13. Butler, L. A. "A Vulnerability Assessment of the Appliqué Computer." ARL-TR-1528, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, 1997.

14. Spafford, E. H. "The Internet Worm: Crisis and Aftermath." *Communications of the ACM,* vol. 32, no. 6, pp. 678–687, June 1989.

The following Internet "Requests for Comments" (RFCs) are available through `http://info.internet.isi.edu/1/in-notes/rfc`.

[RFC-759] Postel, J. *Internet Message Protocol.* 1 August 1980.

[RFC-768] Postel, J. *User Datagram Protocol.* 28 August 1980.

[RFC-783] Sollins, K. R. *TFTP Protocol (revision 2).* 1 June 1981.

[RFC-791] Postel, J. *Internet Protocol.* 1 September 1981.

[RFC-792] Postel, J. *Internet Control Message Protocol.* 1 September 1981.

[RFC-793] Postel, J. *Transmission Control Protocol.* 1 September 1981.

[RFC-826] Plummer, D. C. *Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware.* 1 November 1982.

[RFC-1034] Mockapetris, P. V. *Domain names — concepts and facilities.* 1 November 1987.

[RFC-1035] Mockapetris, P. V. *Domain names — implementation and specification.* 1 November 1987.

[RFC-1157] Case, J. D., M. Fedor, M. L. Schoffstall, and C. Davin. *Simple Network Management Protocol (SNMP).* 1 May 1990.

[RFC-1213] McCloghrie, K., and M. T. Rose. *Management Information Base for network management of TCP/IP-based internets: MIB-II.* 1 March 1991.

[RFC-1332] McGregor, G. *The PPP Internet Protocol Control Protocol (IPCP).* May 1992.

[RFC-1351] Davin, J., J. Galvin, and K. McCloghrie. *SNMP Administrative Model.* July 1992.

[RFC-1352] Galvin, J., K. McCloghrie, and J. Davin. *SNMP Security Protocols.* July 1992.

[RFC-1353] McCloghrie, K., J. Davin, and J. Galvin. *Definitions of Managed Objects for Administration of SNMP Parties.* July 1992.

[RFC-1441] Case, J., K. McCloghrie, M. Rose, and S. Waldbusser. *Introduction to version 2 of the Internet-standard Network Management Framework.* April 1993.

[RFC-1445] Galvin, J., and K. McCloghrie. *Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2).* J. Galvin and K. McCloghrie, April 1993.

[RFC-1446] Galvin, J., and K. McCloghrie. *Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2).* April 1993.

[RFC-1447] McCloghrie, K., and J. Galvin. *Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2).* April 1993.

[RFC-1451] Case, J., K. McCloghrie, M. Rose, and S. Waldbusser. *Manager-to-Manager Management Information Base.* April 1993.

[RFC-1661] Simpson, W. (ed.). *The Point-to-Point Protocol (PPP).* July 1994.

[RFC-1825] Atkinson, R. *Security Architecture for the Internet Protocol.* August 1995.

[RFC-1826] Atkinson, R. *IP Authentication Header.* August 1995.

[RFC-1827] Atkinson, R. *IP Encapsulating Security Payload (ESP).* August 1995.

[RFC-1828] Metzger, P., and W. Simpson. *IP Authentication using Keyed MD5.* August 1995.

[RFC-1829] Karn, P., P. Metzger, and W. Simpson. *The ESP DES–CBC Transform.* August 1995.

[RFC-1883] Deering, S. and R. Hinden. *Internet Protocol, Version 6 (IPv6) Specification.* December 1995.

[RFC-1902] Case, J., K. McCloghrie, M. Rose, and S. Waldbusser. *Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2).* January 1996.

[RFC-1903] Case, J., K. McCloghrie, M. Rose, and S. Waldbusser. *Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2).* January 1996.

[RFC-1904] Case, J., K. McCloghrie, M. Rose, and S. Waldbusser. *Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2).* January 1996.

[RFC-1905] Case, J., K. McCloghrie, M. Rose, and S. Waldbusser. *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2).* January 1996.

[RFC-1906] Case, J., K. McCloghrie, M. Rose, and S. Waldbusser. *Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2).* January 1996.

[RFC-1907] Case, J., K. McCloghrie, M. Rose, and S. Waldbusser. *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2).* January 1996.

[RFC-1908] Case, J., K. McCloghrie, M. Rose, and S. Waldbusser. *Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework.* January 1996.

[RFC-1909] McCloghrie, K. *An Administrative Infrastructure for SNMPv2.* February 1996.

[RFC-1910] Waters, G. *User-based Security Model for SNMPv2.* February 1996.

[RFC-2153] Simpson, W. *PPP Vendor Extensions.* May 1997.

[RFC-2328] Moy, J. *OSPF Version 2.* April 1998.

INTENTIONALLY LEFT BLANK.

NO. OF COPIES ORGANIZATION

2 DEFENSE TECHNICAL INFORMATION CENTER
DTIC DDA
8725 JOHN J KINGMAN RD
STE 0944
FT BELVOIR VA 22060-6218

1 HQDA
DAMO FDQ
DENNIS SCHMIDT
400 ARMY PENTAGON
WASHINGTON DC 20310-0460

1 OSD
OUSD(A&T)/ODDDR&E(R)
R J TREW
THE PENTAGON
WASHINGTON DC 20301-7100

1 DPTY CG FOR RDE HQ
US ARMY MATCOM
AMCRD
MG BEAUCHAMP
5001 EISENHOWER AVE
ALEXANDRIA VA 22333-0001

1 INST FOR ADVNCD TCHNLGY
THE UNIV OF TEXAS AT AUSTIN
PO BOX 202797
AUSTIN TX 78720-2797

1 DARPA
B KASPAR
3701 N FAIRFAX DR
ARLINGTON VA 22203-1714

1 NAVAL SURFACE WARFARE CTR
CODE B07 J PENNELLA
17320 DAHLGREN RD
BLDG 1470 RM 1101
DAHLGREN VA 22448-5100

1 US MILITARY ACADEMY
MATH SCI CTR OF EXCELLENCE
DEPT OF MATHEMATICAL SCI
MDN A MAJ DON ENGEN
THAYER HALL
WEST POINT NY 10996-1786

NO. OF COPIES ORGANIZATION

1 DIRECTOR
US ARMY RESEARCH LAB
AMSRL CS AL TA
2800 POWDER MILL RD
ADELPHI MD 20783-1145

3 DIRECTOR
US ARMY RESEARCH LAB
AMSRL CI LL
2800 POWDER MILL RD
ADELPHI MD 20783-1145

ABERDEEN PROVING GROUND

4 DIR USARL
AMSRL CI LP (305)

NO. OF COPIES ORGANIZATION

2 DCS FOR OPERATIONS & PLANS
DAMO ADO
499 ARMY PENTAGON
WASHINGTON DC 20310-0400

2 DIRECTOR
US ARMY RESEARCH LAB
AMSRL SL EI
A BARNES
FT MONMOUTH NJ 07703

ADELPHI

20 DIR USARL
AMSRL IS
P EMMERMAN
J GANTT
R SLIFE
AMSRL IS TA
D GWYN (4 CP)
G CIRINCIONE
J GOWENS
H HARRELSON
R HASENAUER
B LUU
A MARK
B SADLER
L SADLER
A SWAMI
R TOBIN
D TORRIERI
G TRAN
LTC P WALCZAK

NO. OF COPIES ORGANIZATION

ABERDEEN PROVING GROUND

14 DIR USARL
AMSRL SL B
L BUTLER
AMSRL IS CI
B BROOME
AMSRL IS TP
F BRUNDICK
H CATON
S CHAMBERLAIN
A COOPER
G HARTWIG
M LOPEZ
L MARVEL
C RETTER (4 CP)
C SARAFIDIS

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 1998	Final, 1 Oct 95 - 10 Dec 96

4. TITLE AND SUBTITLE

Vulnerability Assessment of the InterNetwork Controller (INC)

5. FUNDING NUMBERS

622120.H16

6. AUTHOR(S)

Charles Retter and Douglas Gwyn

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Research Laboratory
ATTN: AMSRL-IS-CI
Aberdeen Proving Ground, MD 21005-5067

8. PERFORMING ORGANIZATION REPORT NUMBER

ARL-MR-412

9. SPONSORING/MONITORING AGENCY NAMES(S) AND ADDRESS(ES)

10.SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The Tactical Internet (TI) provides a reliable digital communications infrastructure for Task Force XXI at brigade level and below. The InterNetwork controller (INC) performs routing and protocol conversion of data traffic within the TI, so its vulnerabilities could have significant adverse effects on the flow and content of data communications within the TI. This report summarizes the results of a study of potential "information warfare" vulnerabilities of the INC's interfaces, configuration, protocols, procedures, and policies.

14. SUBJECT TERMS

tactical, internet, vulnerability, INC, information warfare

15. NUMBER OF PAGES

27

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

INTENTIONALLY LEFT BLANK.

USER EVALUATION SHEET/CHANGE OF ADDRESS

This Laboratory undertakes a continuing effort to improve the quality of the reports it publishes. Your comments/answers to the items/questions below will aid us in our efforts.

1. ARL Report Number/Author ARL-MR-412 (Retter) Date of Report September 1998

2. Date Report Received _____

3. Does this report satisfy a need? (Comment on purpose, related project, or other area of interest for which the report will be used.) _____

4. Specifically, how is the report being used? (Information source, design data, procedure, source of ideas, etc.) _____

5. Has the information in this report led to any quantitative savings as far as man-hours or dollars saved, operating costs avoided, or efficiencies achieved, etc? If so, please elaborate. _____

6. General Comments. What do you think should be changed to improve future reports? (Indicate changes to organization, technical content, format, etc.) _____

CURRENT ADDRESS

_____
Organization

_____
Name E-mail Name

_____
Street or P.O. Box No.

_____
City, State, Zip Code

7. If indicating a Change of Address or Address Correction, please provide the Current or Correct address above and the Old or Incorrect address below.

OLD ADDRESS

_____
Organization

_____
Name

_____
Street or P.O. Box No.

_____
City, State, Zip Code

(Remove this sheet, fold as indicated, tape closed, and mail.)
(DO NOT STAPLE)

DEPARTMENT OF THE ARMY

OFFICIAL BUSINESS

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL
FIRST CLASS PERMIT NO 0001,APG,MD

POSTAGE WILL BE PAID BY ADDRESSEE

DIRECTOR
US ARMY RESEARCH LABORATORY
ATTN AMSRL IS CI
ABERDEEN PROVING GROUND MD 21005-5067